

CLAIMS

1. A method comprising:
deriving a secret that is unique to a game console running a particular game title; and
establishing a secure communication link between multiple game consoles over a local area network using the secret.
2. A method as recited in claim 1, wherein the deriving comprises deriving the secret from data stored in the game console and data associated with the particular game title.
3. A method as recited in claim 1, wherein the deriving comprises:
retrieving a console-based key from the game console and a title-based key associated with the particular game title; and
deriving the secret from the console-based key and the title-based key.
4. A method as recited in claim 1, wherein the establishing comprises:
discovering whether another game console on the local area network is hosting the particular game title; and
exchanging secure communication keys between the multiple game consoles to facilitate secure multi-console play of the particular game title over the local area network.

1 5. A method as recited in claim 1, wherein the establishing comprises
2 establishing a secure communication link over an Ethernet segment using the
3 secret.

4
5 6. A method comprising:
6 generating at least one key that is secret to an authentic gaming system
7 running an authentic game title;
8 discovering whether another gaming system on a common local area
9 network is hosting the game title; and
10 establishing a secure communication link between multiple gaming systems
11 to facilitate multi-system play of the game title over the local area network.

12
13 7. A method as recited in claim 6, wherein the generating comprises:
14 retrieving a console-based key from the gaming system and a title-based
15 key associated with the game title; and
16 deriving the key from the console-based key and the title-based key.

17
18 8. A method as recited in claim 6, wherein the discovering comprises
19 broadcasting, over the local area network, a request to join in playing the game
20 title being hosted by another gaming system.

21
22 9. A method as recited in claim 8, wherein the discovering comprises
23 receiving a broadcast reply, over the local area network, from the gaming system
24 that is hosting the game title.
25

1 **10.** A method as recited in claim 6, wherein the discovering comprises:
2 cryptographically encoding, using a generated key, a request to join in
3 playing the game title being hosted by another gaming system; and
4 broadcasting the request over the local area network.

5
6 **11.** A method as recited in claim 6, wherein the discovering comprises
7 broadcasting a request over an Ethernet segment.

8
9 **12.** A method as recited in claim 6, wherein the establishing comprises
10 exchanging secure communication keys between the multiple game consoles to
11 facilitate multi-console play of the particular game title over the local area
12 network.

13
14 **13.** In a networked gaming environment where multiple game consoles
15 are connected via a local area network, a method comprising:

16 broadcasting, from a client game console over a local area network, a
17 request to join in playing a game title in a network gaming session being hosted by
18 a host game console, the request containing a secret that is unique to the client
19 game console running the game title; and

20 broadcasting, from the host game console over the local area network, a
21 reply to the request, the reply containing information that can be used to establish
22 a secure communication link.

1 **14.** A method as recited in claim 13, further comprising deriving the
2 secret from data stored in the client game console and data associated with the
3 game title.

4
5 **15.** A method as recited in claim 13, wherein the local area network
6 comprises an Ethernet segment.

7
8 **16.** A method comprising:
9 retrieving a console-based key stored on a game console;
10 retrieving a title-based key associated with a game title running on the
11 game console; and
12 deriving one or more keys from the console-based key and the title-based
13 key.

14
15 **17.** A method as recited in claim 16, wherein the deriving comprises
16 computing a hashing function on a concatenation of the console-based key and the
17 title-based key.

18
19 **18.** One or more computer-readable media comprising computer-
20 executable instructions that, when executed, perform the method as recited in
21 claim 16.

22
23 **19.** In a networked gaming environment where multiple game consoles
24 are connected via a local area network, a method comprising:
25

1 creating a request to join in playing a game title being hosted by a host
2 game console on the local area network;
3 broadcasting the request over the local area network;
4 receiving a reply from the host game console, the reply containing one or
5 more session keys; and
6 using the session keys from the reply to facilitate future secure
7 communication with the host game console.

8
9 **20.** A method as recited in claim 19, wherein the broadcasting
10 comprises broadcasting the request over an Ethernet segment.

11
12 **21.** A method as recited in claim 19, further comprising
13 cryptographically encoding the request prior to the broadcasting.

14
15 **22.** A method as recited in claim 19, wherein the receiving comprises
16 listening for a reply that is broadcast from the host game console over the local
17 area network.

18
19 **23.** A method as recited in claim 22, wherein the broadcast reply is
20 cryptographically encoded, and further comprising cryptographically decoding the
21 reply.

22
23 **24.** One or more computer-readable media comprising computer-
24 executable instructions that, when executed, perform the method as recited in
25 claim 19.

1
2 **25.** In a networked gaming environment where multiple game consoles
3 are connected via a local area network and at least two game consoles are playing
4 a same game title, a method comprising:

5 forming an initial packet that contains first data used to derive a
6 cryptographic key;

7 computing a first hash digest of the initial packet;

8 sending the initial packet and the first hash digest to another game console
9 on the local area network that is playing the same game title;

10 receiving a reply packet from the other game console, the reply packet
11 including a second hash digest and second data;

12 authenticating the reply packet using the second hash digest; and

13 deriving one or more security association keys from the first and second
14 data, the security association keys being used to secure communication between
15 the multiple consoles.

16
17 **26.** One or more computer-readable media comprising computer-
18 executable instructions that, when executed, perform the method as recited in
19 claim 25.

20
21 **27.** In a networked gaming environment where multiple game consoles
22 are connected via a local area network, a method comprising:

23 retrieving a console-based key from a first game console and a title-based
24 key associated with a game title running on the first game console;

1 deriving at least one cryptographic key from the console-based key and the
2 title-based key;
3 creating, at a first console, a request to join in playing the game title being
4 hosted by a second game console on the local area network;
5 cryptographically encoding the request using the cryptographic key;
6 broadcasting the request over the local area network;
7 cryptographically decoding the request, at the second game console, using
8 the cryptographic key;
9 generating, at the second game console, a reply that contains at least one
10 session key;
11 cryptographically encoding the reply using the cryptographic key;
12 broadcasting the reply over the local area network;
13 cryptographically decoding the reply, at the first game console, using the
14 cryptographic key;
15 exchanging packets between the first and second game consoles, the
16 packets being protected using the session key and containing data used to derive at
17 least one security association key; and
18 establishing a secure communication link between the first and second
19 game consoles using the security association keys to facilitate secure multi-
20 console play of the game title.

21
22 **28.** A method as recited in claim 27, wherein the deriving comprises
23 computing a hashing function on a concatenation of the console-based key and the
24 title-based key.
25

1 **29.** A method as recited in claim 27, wherein:

2 the deriving comprises computing an encryption key and a signature key;

3 and

4 the encoding of the request comprises encrypting the request using the
5 encryption key to form an encrypted request and digitally signing the encrypted
6 request using the signature key.

7
8 **30.** A method as recited in claim 27, wherein the exchanging comprises:

9 forming, at one of the first or second game consoles, a packet that contains
10 the data used to derive the security association key;

11 computing a hash digest of the packet;

12 sending the packet and the hash digest to the other of the first or second
13 game consoles; and

14 authenticating the packet using the hash digest at the other first or second
15 game consoles.

16
17 **31.** A method as recited in claim 27, wherein the data used to derive the
18 security association key comprises values used by a cryptographic Diffie-Hellman
19 function.

20
21 **32.** One or more computer-readable media comprising computer-
22 executable instructions that, when executed, perform the method as recited in
23 claim 27.

1 **33.** In a networked gaming environment where multiple game consoles
2 are connected via a local area network, a method comprising:
3 retrieving a console-based key from a first game console and a title-based
4 key associated with a game title running on the first game console;
5 deriving at least one cryptographic key from the console-based key and the
6 title-based key;
7 creating a request to join in playing the game title being hosted by another
8 game console on the local area network;
9 encoding the request using the cryptographic key;
10 broadcasting the request over the local area network;
11 receiving a reply from a host game console, the reply containing at least
12 one session key;
13 exchanging packets with the host game console, the packets being protected
14 using the session key and containing data used to derive at least one security
15 association key; and
16 establishing a secure communication link with the host game console using
17 the security association key.

18
19 **34.** A method as recited in claim 33, wherein the receiving comprises
20 listening for a reply that is broadcast from the host game console over the local
21 area network.

22
23 **35.** One or more computer-readable media comprising computer-
24 executable instructions that, when executed, perform the method as recited in
25 claim 33.

1
2 **36.** In a networked gaming environment where multiple game consoles
3 are connected via a local area network, a method comprising:

4 retrieving a console-based key from a first game console and a title-based
5 key associated with a game title running on the first game console;

6 deriving at least one cryptographic key from the console-based key and the
7 title-based key;

8 receiving a request to join in playing the game title from another game
9 console on the local area network;

10 cryptographically decoding the request using the cryptographic key;

11 generating a reply that contains at least one session key;

12 encoding the reply using the cryptographic key;

13 sending the reply over the local area network;

14 exchanging packets with the other game console, the packets being
15 protected using the session key and containing data used to derive at least one
16 security association key; and

17 establishing a secure communication link with the other game console
18 using the security association key.

19
20 **37.** A method as recited in claim 33, wherein the sending comprises
21 broadcasting the reply over the local area network.

22
23 **38.** One or more computer-readable media comprising computer-
24 executable instructions that, when executed, perform the method as recited in
25 claim 33.

1
2 **39.** A computer-readable medium for a game console comprising
3 computer-executable instructions that, when executed, direct the game console to:
4 obtain a first key stored in memory of the game console and a second key
5 associated with a game title running on the game console; and
6 derive one or more keys from the first and second keys.
7

8 **40.** A computer-readable medium for a game console comprising
9 computer-executable instructions that, when executed, direct the game console to:
10 encrypt a request to join in playing a game title being hosted by a remote
11 host game console on a local area network;
12 digitally sign the request;
13 broadcast the request over the local area network;
14 listen for at least one broadcast reply from the host game console;
15 upon receipt of the reply, extract at least one session key from the reply for
16 use in facilitating future communication with the host game console;
17 form an initial packet that contains first data used to derive a cryptographic
18 key;
19 compute a first hash digest of the initial packet using the session key;
20 send the initial packet and the first hash digest to the host game console;
21 listen for a reply packet from the host game console, the reply packet
22 including a second hash digest and second data;
23 authenticate the reply packet using the session key and the second hash
24 digest; and
25

1 derive at least one security association key from the first and second data,
2 the security association keys being used to secure communication with the host
3 game console.

4
5 **41.** A computer-readable medium for a game console comprising
6 computer-executable instructions that, when executed, direct the game console to:

7 receive a request from a remote game console on a local area network, the
8 request seeking network play of a game title;

9 authenticate the request as being generated by an authentic game console
10 running an authentic version of the game title;

11 decode the request;

12 determine whether to allow the remote game console to play;

13 in an event the remote game console is allowed to play, create a reply with
14 containing at least one session key;

15 encrypt and digitally sign the reply;

16 send the reply to the remote game console;

17 receive an initial packet directly from the remote game console, the initial
18 packet containing first data used to derive a cryptographic key;

19 authenticate the initial packet using the session key;

20 form a response packet holding second data used to derive a cryptographic
21 key;

22 send the response packet to the remote game console; and

23 derive at least one security association key from the first and second data,
24 the security association keys being used to secure communication with the remote
25 game console.

1
2 42. A computer-readable medium as recited in claim 41, further
3 comprising computer-executable instructions that, when executed, direct the game
4 console to broadcast the response packet over the local area network.
5

6 43. A game console, comprising:
7 a memory to store a first key;
8 a game title configured to execute on the game console, the game title
9 having an associated second key; and
10 a processor coupled to the memory, the processor being configured to
11 derive at least one cryptographic keys from the first and second keys.
12

13 44. A game console as recited in claim 43, wherein the memory
14 comprises a read only memory.
15

16 45. A game console as recited in claim 43, wherein the processor is
17 configured to compute a hash function of the first and second keys.
18

19 46. A game console as recited in claim 43, wherein the processor is
20 further configured to discover another game console on a local area network that is
21 hosting the game title.
22

23 47. A game console as recited in claim 43, wherein the processor is
24 further configured to use the cryptographic key to establish a secure
25 communication link with a remote game console over a local area network.

1
2 **48.** A game console, comprising:

3 a memory; and

4 a processor coupled to the memory and configured to generate at least one
5 key that is secret to the game console when running an authentic game title, the
6 processor being further configured to discover, using the key, a host game console
7 on a common local area network that is hosting the game title and to establish a
8 secure communication link with the host game console over the local area
9 network.
10

11 **49.** A game console as recited in claim 48, wherein the processor is
12 configured to derive the key from data stored in the memory and data associated
13 with the authentic game title.
14

15 **50.** A game console as recited in claim 48, wherein the processor is
16 further configured to discover a host game console by creating a request to join in
17 playing the game title and broadcasting the request over the local area network.
18

19 **51.** A game console as recited in claim 48, wherein the processor
20 establishes the secure communication link by exchanging data with the host game
21 console that can be used to derive a cryptographic key.
22

23 **52.** A system, comprising:

24 first and second game consoles with network connections to facilitate
25 connection to a local area network, the first and second game consoles running a

1 same game title and being configured to generate identical keys by virtue of
2 running the same game title; and

3 the first game console being configured to discover the second game
4 console by broadcasting messages over the local area network, the messages being
5 secured by the keys.

6
7 **53.** A system as recited in claim 52, where in the first and second game
8 consoles are configured to establish a secure communication link over the local
9 area network by exchanging data used to derive a cryptographic key.

10
11 **54.** A system as recited in claim 52, where in the local area network
12 comprises an Ethernet segment.
13
14
15
16
17
18
19
20
21
22
23
24
25